単調並べ換え関数について(アルゴリズムと計算量理論)

AUTHOR(S):

神保, 秀司; 佐々木, 宏平; 山本, 佳典; 丸岡, 章

CITATION:

神保, 秀司 ...[et al]. 単調並べ換え関数について(アルゴリズムと計算量理論). 数理解析研究所講究録 1995, 906: 96-103

ISSUE DATE:

1995-04

URL:

http://hdl.handle.net/2433/59456

数理解析研究所講究録
906巻 1995年 96-103

単調並べ換え関数について

神保 秀司 (Shuji Jimbo), 佐々木 宏平 (Kohei Sasaki),
山本 佳典 (Yoshinori Yamamoto), 丸岡 章 (Akira Maruoka)
(東北大学・情報科学研究科)

1 はじめに

n は正整数を表す. 2 つの n 次元のベクトル $(x_1, x_1, \ldots, x_n)$ と $(y_1, y_2, \ldots, y_n)$ に対して, $x_1 \leq y_1$, $x_2 \leq y_2$, $\ldots$, $x_n \leq y_n$ が全て成立することを, $(x_1, x_1, \ldots, x_n) \leq (y_1, y_2, \ldots, y_n)$ と表す. 単調並べ換え関数とは, 次の性質を持つ関数 $f : \{0,1\}^n \to \{0,1\}^n$ である:

1. f は単調である. つまり, 任意の $x \in \{0,1\}^n$ および $y \in \{0,1\}^n$ に対して, $x \leq y$ ならば $f(x) \leq f(y)$ が成立する.

2. f の出力は, 入力の成分を並べ換えたものになっている. つまり, 任意の $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ に対して,

$$f(x_1, x_2, \ldots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

を満足する $\{1, 2, \ldots, n\}$ 上の置換 σ が存在する.

整列 (sorting) 関数は, 単調並べ換え関数の典型例である. 整列を実現する各種のアルゴリズムが研究されているが, そこで使われる計算モデルの中に, 比較器回路網がある. 古くから研究されているモデルで, 入力を 0 と 1 に限定した場合, 強い制約が付けられた単調論理回路と見なせる. Kunuth[4] は, 整列およびそれに類似した問題を比較器回路網で解くことについて, 数多くの演習問題も含めて詳しく記述している. そこでは, 図 1 にあるように, 比較器回路網は左右に延びる入力数と同じ本数の横線とそれらの内の 2 本を結ぶ比較器と呼ばれる上下方向の線分複数個で表されている. 一般に, 比較器には向きが定められていて, 単なる線分ではなく矢印付きの

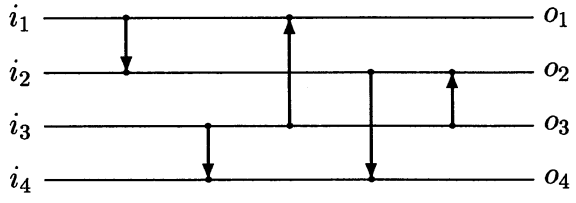

図 1: 比較器回路網の図示

線分として表されることもあるが, 単なる線分として表されたものは, 下向きと考える. 入力されたデータは, 左から右に横線の上を流れて行き, 比較器 (上下方向の線分) に出会うと, その比較器のもう一方の端点に出会ったデータと大小に関する比較が為され, その大きい方が比較器の先の端に, 小さい方が本の端に来るように, 必要なら 2 つのデータの入れ換えが為され, その後 2 つのデータはそれぞれ, 比較器の端点を通る横線の上を右に流れて行く. 比較器回路網への入力

が 0 あるいは 1 に限定されていれば, 単一の比較器は, 1 個の論理和素子と 1 個の論理積素子で実現できるので, 比較器回路網が計算する論理関数は, 比較器回路網の中の各比較器をそのような等価な論理回路で置き換えて得られる単調論理回路によって計算される. 尚, このように, 比較器回路網は強い制約が付けられたモデルではあるが, 整列の計算に関しては, 他の計算モデルと比べて能力的に著しく劣ることはない. Ajtai ら [1, 2] は, 比較の回数, つまり比較器の個数が定数倍の違いを除いて最適な (入力数を n としたとき $O(n \log n)$) 整列回路網 (sorting network, 整列を計算する比較器回路網) を与えている. また, その整列回路網の深さは, $O(\log n)$ である.

上に述べた比較器回路網の定義からわかるように, 整列関数に限らず比較器回路網が計算する関数は全て単調並べ換え関数である. 以下, 比較器回路網が計算する関数を比較器回路網関数と呼ぶ. 論理和と論理積だけを基本素子とする論理回路が計算する関数の族が単調論理関数の族と一致することからの類推により, 筆者らは, 当初比較器回路網関数の族と単調並べ換え関数の族が一致することを予想したが, その予想は, 4 変数の場合の簡単な反例の発見によって覆された. その反例の一つは, 次の一連の式により定まる関数 f である.

$$
\begin{array}{ll}
f(0,0,0,0) = (0,0,0,0), & f(1,0,0,0) = (1,0,0,0), \\
f(0,1,0,0) = (1,0,0,0), & f(1,1,0,0) = (1,1,0,0), \\
f(0,0,1,0) = (1,0,0,0), & f(1,0,1,0) = (1,1,0,0), \\
f(0,1,1,0) = (1,0,1,0), & f(1,1,1,0) = (1,1,1,0), \\
f(0,0,0,1) = (1,0,0,0), & f(1,0,0,1) = (1,0,1,0), \\
f(0,1,0,1) = (1,0,1,0), & f(1,1,0,1) = (1,1,1,0), \\
f(0,0,1,1) = (1,1,0,0), & f(1,0,1,1) = (1,1,1,0), \\
f(0,1,1,1) = (1,1,1,0), & f(1,1,1,1) = (1,1,1,1).
\end{array}
$$

この関数 f は, 計算機を使った調査により得られた. 尚, 比較器回路網に関する理論的研究に計算機を導入した最近の例としては, Parberry[5] によるものが挙げられる. そこでは, 深さ 6 の 9 入力整列回路網は存在しないことが示されている.

筆者らは, 次の二つの問題を単調並べ換え関数およびその重要な部分族である比較器回路網関数に関する基本的な問題として取り上げ, 当面の目標としている.

1. 単調並べ換え関数をその中の関数の合成だけで全て実現できる単調並べ換え関数の最小の部分族は何か.

2. $\{0,1\}^n$ から $\{0,1\}^n$ への関数の関数表が与えられたとき, その関数が比較器回路網で計算できるか否かを関数表のサイズ $n2^n$ の多項式程度の時間で判定するアルゴリズムは存在するか.

問題 1 は, 次のように言い換えることができる. 「比較器回路網の基本素子集合を変更して任意の単調並べ換え関数を計算できるようにするとき, その基本素子集合をどこまで小さくできるか. 」

本論文では, 上で提案した問題の内, 問題 1 に関する研究により得られた結果について述べる.

2 準備

前節で述べた問題自身およびそれらに対する筆者らの手法を述べる為に, いくつかの概念を定義する.

$\{1,2,\ldots,n\}$ 上の置換 ρ と, 各 $(x_1,x_2,\ldots,x_n)\in\{0,1\}^n$ に $(x_{\rho(1)},x_{\rho(2)},\ldots,x_{\rho(n)})$ を対応させる単調並べ換え関数を同一視し, この単調並べ換え関数も ρ と表す.

単調並べ換え関数 $f:X\to Y$ と $g:Y\to Z$ に対して, 単調並べ換え関数 $g\circ f:X\to Z$ は, g と f の合成関数, 即ち任意の $x\in X$ に対して, $(g\circ f)(x)=g(f(x))$ が成立する関数を表す. 関数の合成に関して結合法則が成立するので, 単調並べ換え関数 f,g,h に対して, $g\circ f$ 及び $h\circ g$ がどちらも定義できれば, $h\circ(g\circ f)=(h\circ g)\circ f$ が成立する.

関数 $f:\{0,1\}^n\to\{0,1\}^n$ に対して, 関数 $f_1,f_2,\ldots,f_n:\{0,1\}^n\to\{0,1\}$ が f の出力となっていること, つまり, 任意の $x\in\{0,1\}^n$ に対して, $f(x)=(f_1(x),f_2(x),\ldots,f_n(x))$ となっていることを $f=(f_1,f_2,\ldots,f_n)$ と表す.

定義 1 単調並べ換え関数 $f=(f_1,f_2,\ldots,f_n):\{0,1\}^n\to\{0,1\}^n$ に対して, 2 つ以上の変数に依存する出力を $f_{j_1},f_{j_2},\ldots,f_{j_k}$ としたとき, 単調並べ換え関数の定義より, $i_1,i_2,\ldots,i_k\in\{1,2,\ldots,n\}$ が存在して, $f_{j_1}(x_1,x_2,\ldots,x_n)$, $f_{j_2}(x_1,x_2,\ldots,x_n)$, $\ldots$, $f_{j_k}(x_1,x_2,\ldots,x_n)$ は, 全て $(x_{i_1},x_{i_2},\ldots,x_{i_k})$ で決定する. 但し, $i_1<i_2<\cdots<i_k$ とする. このようにして得られる $\{0,1\}^k$ から $\{0,1\}^k$ への単調並べ換え関数を $\tilde{f}$ と表す.

定義 2 2 つの単調並べ換え関数 f と g が同値であるとは, $\tilde{f}$ と $\tilde{g}$ の入力数が等しく, それを k とおいて, k 変数の 2 つの置換 ρ,σ が存在して, $\tilde{g}=\rho\circ\tilde{f}\circ\sigma$ となることと定義し, $f\equiv g$ と表す.

この定義から, 単調並べ換え関数 f と g の入力数が等しい場合, $f=\rho\circ g\circ\sigma$ となる置換 ρ と σ が存在すれば, f と g は同値である.

このように 2 つの単調並べ換え関数の間の同値関係を定義すれば, 第 1 節で挙げた問題 1 は, 次のように書き直すことにより, より自然な形になる.

> **問題 1′** 単調並べ換え関数をその中の関数と同値な関数の合成だけで全て実現できる単調並べ換え関数の最小の部分族は何か.

単調並べ換え関数を有限個の基本素子から成る拡張された比較器回路網で実現できるかという問題は, 上の問題における単調並べ換え関数の最小の部分族は有限かと言うことができる. 以下では, 問題 1′ の解となる関数の族を基本素子集合と呼ぶことにする.

同値な単調並べ換え関数の間に本質的な働きの違いはないので, ある単調並べ換え関数が比較器回路網で計算することができれば, その関数と同値な全ての関数は比較器回路網で計算できる. また, 計算機実験において単調並べ換え関数の関数表を表す大量のデータを蓄えておく場合, 各同値類に対して, 適当な代表元のみを蓄えておくようにすれば記憶領域を節約できる.

n 変数の 2 つの単調並べ換え関数 f と g に対して, n 変数の置換 ρ が存在て, $f=\rho\circ g$ となっているとき, f と g は, 「出力に関して」同値であると言うことにする. この定義からわかるように, f と g が出力に関して同値ならば同値であるが, 逆は必ずしも成立しない. 単調並べ

換え関数 f の関数表が与えられたとき, f が属する出力に関する同値類の代表元を次に述べるように定めると, その代表元を容易に求めることができる. 従って, 2 つの単調並べ換え関数が出力に関して同値であるか否かは容易に判定できる. その代表元とは, $x = (1, 1, \ldots, 1, 0, 0, \ldots, 0)$ の形の $n+1$ 個の入力に x 自身を対応付ける単調並べ換え関数であり, それを元の単調並べ換え関数の (そしてその単調並べ換え関数が属する同値類の) 出力に関する標準形と呼ぶ. 比較器回路網関数の出力に関する標準形は, 全ての比較器の向きが等しい比較器回路網で計算することができる. このような比較器回路網を標準回路網と呼ぶ. 筆者らは, 5 変数以下の全ての単調並べ換え関数の出力に関する標準形を求めるこに成功した. 尚, 与えられた 2 つの単調並べ換え関数が同値であるか否かの容易な判定方法は, 現在筆者らには知られていない.

n 変数の (i, j)-比較器とは, 横線 i と 横線 j を結ぶ単一の比較器だけからなる比較器回路網関数であり, その比較器の向きは i から j へである. より厳密には, (i, j)-比較器は, 任意の $x = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ に対して, $f(x) = (y_1, y_2, \ldots, y_n)$ と表したとき, $y_i = x_i \wedge x_j$ かつ $y_j = x_i \vee x_j$ が成立する単調並べ換え関数 f である. 尚, 単に「比較器」という言葉を単調並べ換え関数の意味で使ったときは, 何らかの i および j が存在して, (i, j)-比較器と表される単調並べ換え関数を意味することにする.

同一の定義域を持ち半順序集合の中に値を取る関数 f と g に対して, 任意の入力 x に対して $f(x) \leq g(x)$ が成立していれば, $f \leq g$ と表す.

定義 3 i, および j は高々 n の正整数とする. 単調並べ換え関数 $f = (f_1, f_2, \ldots, f_n)$ が (i, j)-連結であるとは, $\{0,1\}^n = \{0,1\}^n$ を頂点の集合とする超立方体 (hypercube) $\mathcal{H}_n$ の頂点の部分集合 $\{x \in \{0,1\}^n \mid f_i(x) \neq f_j(x)\}$ により誘導された部分グラフが連結であることと定義する. $\mathcal{H}_n$ は無向グラフであり, その辺の集合は丁度一つの成分が異なる二つの頂点を結ぶ辺からなる.

定義 4 n を正整数とする. 高々 n の任意の整数 i および j に対して, $f_i \leq f_j$ あるいは $f_i \geq f_j$ ならば (i, j)-連結であるという条件を満たす単調並べ換え関数 $f = (f_1, f_2, \ldots, f_n)$ 全てから成る集合を $\mathcal{G}_n$ と表す.

(i, j)-連結という概念に関して次の定理が成立する.

定理 1 $\mathcal{G}_n$ に属する単調並べ換え関数は比較器回路網では計算できない. また, n 変数単調並べ換え関数で比較器回路網で計算できないものが存在するならば, $\mathcal{G}_n$ は空ではない.

この定理は, 引き続く定理 2 および命題 1 から導かれる.

定理 2 $f = (f_1, f_2, \ldots, f_n)$ を単調並べ換え関数とし, c を n 変数の (i, j)-比較器とする. このとき, 次の 2 つの命題が成立する.

1. $f_i \leq f_j$ でも $f_i \geq f_j$ でもないならば, $f' = (f'_1, f'_2, \ldots, f'_n) = c \circ f$ は f と同値ではなくかつ f' は (i, j)-連結ではなくかつ $f'_i \leq f'_j$.
2. 逆に, 単調並べ換え関数 $f' = (f'_1, f'_2, \ldots, f'_n)$ が $f'_i \leq f'_j$ かつ (i, j)-連結でないならば, f' と同値ではない単調並べ換え関数 $f = (f_1, f_2, \ldots, f_n)$ が存在して, $f' = c \circ f$ かつ $f_i \leq f_j$ でも $f_i \geq f_j$ でもない.

入力数 n	全単調並べ換え関数の個数	非回路網関数の個数	$\mathcal{G}_n$ の個数
3	5	0	0
4	39	3	3
5	2028	929	299

表 1: 3 ～ 5 変数の単調並べ換え関数の部分族のサイズ

定理 2 の証明は省略する. 次の命題 1 は, Kunuth[4] の 5.3.4 節の問題 40 およびその解答に書かれている (原論文は Graham[3]).

命題 1 $f = (f_1, f_2, \ldots, f_n)$ を単調並べ換え関数, c を n 変数の (i,j)-比較器, $f' = (f'_1, f'_2, \ldots, f'_n) = c \circ f$ とする. $f_i \leq f_j$ でも $f_i \geq f_j$ でもないならば, $f'_u \leq f'_v$ を満足する二項組 (u,v) の個数は, $f_r \leq f_s$ を満足する二項組 (r,s) の個数よりも真に大きい.

以下に, 定理 1 の証明の概略を述べる.

n 変数単調並べ換え関数 $r = (r_1, r_2, \ldots, r_n)$ に対して, $r_i \leq r_j$ を満足する二項組 (i,j) の個数を $P_{\#}(r)$ と表す.

$\mathcal{G}_n$ に属さずかつ比較器回路網関数ではない n 変数の単調並べ換え関数 f が存在したとする. 何らかの比較器回路網関数 h が存在して, $f = h \circ g$ となるような単調並べ換え関数 $g = (g_1, g_2, \ldots, g_n)$ のうち, $P_{\#}(g)$ が最小のものの一つを g_0 とおく. g_0 は, $\mathcal{G}_n$ に属する. なぜならば, もし g_0 が $\mathcal{G}_n$ に属さないならば, $\mathcal{G}_n$ の定義と定理 2 の 2 より, $P_{\#}(g_0) > P_{\#}(g')$ を満足する単調並べ換え関数 g' が存在することになり, これは, $P_{\#}(g_0)$ の最小性に反する.

3 単調並べ換え関数の個数に対する比較器回路網関数の個数の割合

定理 1 からわかるように, 比較器回路網で計算できない単調並べ換え関数の例を一つ見付けようとするなら, n を何らかの正整数として, $\mathcal{G}_n$ に属する関数を捜せばよい. 計算機を用いた調査により, そのような関数の例として, $\mathcal{G}_4$ に属する関数が最初に発見された. 尚, $\mathcal{G}_3$ は空集合であり, 従って比較器回路網で計算できない 3 変数単調並べ換え関数は存在せず, また, 4 入力の比較器回路網で計算できない単調並べ換え関数は, 全て $\mathcal{G}_4$ に属しかつ $\mathcal{G}_4$ を定義 2 で述べた同値関係で類別したときの同値類の個数は 3 であることが, 計算機を用いた調査によって判明している.

但し, 全ての整数 $n \geq 4$ に対して, 比較器回路網で計算できない n 変数単調並べ換え関数が全て $\mathcal{G}_n$ に属する訳ではないことが, $n = 5$ の場合の調査結果から判明している. 表 1 に, $n = 3, 4, 5$ の場合の, 全ての単調並べ換え関数の個数, 比較器回路網では計算できない単調並べ換え関数の個数, $\mathcal{G}_n$ に属する単調並べ換え関数の個数が載せてある. 但し, この表における個数は, 全て定義 2 で述べた同値関係で類別したときの同値類の個数である.

更に, 筆者らは次の命題を示した.

定理 3 n が増加するにつれて, n 変数単調並べ換え関数全体の個数に対する n 変数比較器回路網関数の個数の割合は 0 に近づく.

定理 3 は, 次に述べる事実に基づいて証明することができる. 詳しい証明は省略する.

$i = \lfloor n/2 \rfloor, j = \lfloor n/2 \rfloor + 1$ とおき, $f = (f_1, f_2, \ldots, f_n)$ とおく. f_i は, 入力中の 1 の個数が i 以上ならば 1 を出力し, そうでなければ 0 を出力するという条件を満たし, f_j は, 入力中の 1 の個数が j 以上ならば 1 を出力し, そうでなければ 0 を出力するという条件を満たすと仮定する. 例えば, 標準整列回路網 (standard sorting network) が計算する関数は, ここでの f の条件を満たす. このとき, 頂点集合 $X = \{x \in \{0,1\}^n \mid f_i(x) = 1 \text{ かつ } f_j(x) = 0\}$ により誘導された n 次元ハイパーキューブ $\mathcal{H}_n$ の部分グラフ G_X の連結成分は, 値が 1 の成分を丁度 i 個持つ $\{0,1\}^n$ に属する単一のベクトルだけからなる孤立点である. そのような孤立点の個数は, $\binom{n}{\lfloor n/2 \rfloor} = \Omega(2^n/\sqrt{n})$ であり, それらは, 全て G_X の連結成分になっている. 従って, (i,j)-比較器を c とおいて, $f = c \circ g$ となる単調並べ換え関数 g の出力に関する標準形の個数は, $2^{\binom{n}{\lfloor n/2 \rfloor}}$ 以上である.

一方, 比較器回路網関数の出力に関する標準形の個数は, 命題 1 より

$$1 + \sum_{i=2}^{\binom{n}{2}} \prod_{j=i}^{\binom{n}{2}} j \leq 2\binom{n}{2}! \leq 2^{n^2 \log_2 n}$$

以下である.

筆者らは, 上で比較器回路網関数の個数を評価したように, 正整数 m および n に対して, 高々 m 変数の単調並べ換え関数と同値な関数だけの合成で得られる n 変数単調並べ換え関数の個数の上界を評価することにより, 次の命題が導かれると予想している.

予想 1 単調並べ換え関数を, その中の関数と同値な関数の合成だけで全て実現できる単調並べ換え関数の有限集合は存在しない.

4 単調並べ換え関数の分解可能性

本節では, 問題 1′ を後略する一つの手段として, 単調並べ換え関数の分解可能性について考察する.

問題 1′ の解である基本素子集合に属する関数は, 比較器を除いて全て, 何らかの正整数 n に対する $\mathcal{G}_n$ に属することは明らかである. 但し, $\mathcal{G}_n$ がそのような関数を含んだからと言って, $\mathcal{G}_n$ が基本素子集合に包含されるとは限らない.

単調並べ換え関数 f が単調並べ換え関数 g と h の冗長でない合成により得られるとは, $f = g \circ h$ かつ $f \neq g$ かつ $f \neq h$ が成立することとする. 単調並べ換え関数 $f \in \mathcal{G}_n$ が, どのような 2 つの単調並べ換え関数 g と h の冗長でない合成によっても得られないならば, f は基本素子集合に属すると言える. この判定の際に, 次に述べる定理 4 を利用して, 冗長でない合成に用いる g と h の範囲を狭めることができる.

定義 5 (単調並べ換え関数の分解可能性) n 変数単調並べ換え関数 f が, 単調並べ換え関数の族 A と B により分解可能であるとは, f が g と h の冗長にならない合成により得られるという条件を満足する $g \in A$ および $h \in B$ が存在することを言う.

尚, f が単調並べ換え関数の族 A と A により分解可能であることを, f が A により分解可能であると言い, f が n 変数単調並べ換え関数により分解可能であることを, 単に f は分解可能であると言う.

$\mathcal{C}_n$ は比較器回路網関数全体から成る族とする. 次の定理は, $\mathcal{G}_n$ に属する関数 f が比較器回路網関数以外の関数全体から成る族により分解可能ならば,

1. f は $\mathcal{G}_n$ により分解可能である.

2. f は $\mathcal{G}_n$ と $\mathcal{C}_n$ により分解可能である.

のどちらかが成立することを主張している.

定理 4 n を正整数とし, f を $\mathcal{G}_n$ に属する関数とする. f_1 と f_2 を比較器回路網で計算できない n 変数単調並べ換え関数とし, $f_1 \neq f$ および $f_2 \neq f$ が成立するとする. このとき, $f = f_2 \circ f_1$ ならば, $g_1 \neq f$ を満たす $g_1 \in \mathcal{G}_n$ および $g_2 \neq f$ を満たす $g_2 \in \mathcal{G}_n$ が存在して $f = g_2 \circ g_1$ が成立するか, あるいは, $g \neq f$ を満たす $g \in \mathcal{G}_n$ および n 変数比較器回路網関数 γ が存在して, $f = g \circ \gamma$ が成立する.

(証明) f_1 は, 適当な比較器回路網関数 C_1 と $f_1' \in \mathcal{G}_n$ によって $f_1 = C_1 \circ f_1'$ と表すことができる (f_1' として, 比較器回路網関数 C_1 が存在して $f = C_1 \circ f_1'$ と表せるもののうち, $P_{\#}(f_1')$ が最小となるものを選べばよい). $f_1 \in \mathcal{G}_n$ のときかつそのときのみ C は恒等関数と同値になる. 同様に, f_2 を比較器回路網関数 C_2 と $f_2' \in \mathcal{G}_n$ によって $f_2 = C_2 \circ f_2'$ と表す.

$f \equiv f_2' \circ C_1 \circ f_1'$ が成立する. なぜなら, そうでないと仮定すると定理 2 の 1 より $f \notin \mathcal{G}_n$ となり, 定理の仮定と矛盾する.

$f \neq f_2'$ が成立する. なぜなら, $f \equiv f_2'$ と仮定すると, $f_2 = C_2 \circ f_2' \neq f \equiv f_2'$ が成立するので, 後に述べる補題 1 より $|f(\boldsymbol{B}^n)| = |f_2'(\boldsymbol{B}^n)| < |f_2(\boldsymbol{B}^n)| \leq |f(\boldsymbol{B}^n)|$ が導かれ矛盾が生じる. 同様に, $f \neq f_1'$ の成立を示すことができる.

$f \equiv f_2' \circ C_1$ ならば, f_2' と同値な $g \in \mathcal{G}_n$ および C_1 と同値な γ をうまく選んで, $f = g \circ \gamma$ と表すことができ, これらの g, γ は定理の条件を満たす. 従って, $f \neq f_2' \circ C_1$ と仮定してよい. $h = f_2' \circ C_1$ とおく. $h \in \mathcal{G}_n$ ならば, $g_2 = h$, $g_1 = f_1'$ とおけば, これらは定理の条件を満たす. 従って, $h \notin \mathcal{G}_n$ と仮定してよい.

h が比較器回路網関数であると仮定すると, $f = h \circ f_1'$ および $f \in \mathcal{G}_n$ より $f \equiv f_1'$ でなければならないが, これは, $f \neq f_1'$ と矛盾する. 従って, h は比較器回路網関数ではないと仮定してよい.

h を比較器回路網関数 C' と $h' \in \mathcal{G}_n$ によって $h = C' \circ h'$ と表す. $f = C' \circ h' \circ f_1'$ より $f \equiv h' \circ f_1'$ が成立する. そうでないと仮定すると, 定理 2 の 1 より $f \notin \mathcal{G}_n$ が導かれ矛盾が生じる. 従って, h' と同値な $g_2 \in \mathcal{G}_n$ と f_1' と同値な $g_1 \in \mathcal{G}_n$ が存在して, $f = g_2 \circ g_1$ が成立する. □

補題 1 f を n 変数単調並べ換え関数 c を比較器とする. $c \circ f$ と f が同値でないならば,

$$|(c \circ f)(\{0,1\}^n)| < |f(\{0,1\}^n)|$$

が成立する.

一般に, 半順序集合 S の部分集合 X に対して, $\{x \in S \mid (\exists y \in X)(y \leq x)\}$ を X の (S における) 上側と呼ぶことにする. 補題 1 は, (i,j)-比較器を c とおき, $f(x) = (f_1(x), f_2(x), \ldots, f_n(x))$

とし, 更に $X = \{x \in \{0,1\}^n \mid f_i(x) = 1 \text{ かつ } f_j(x) = 0\}$ の上側と $Y = \{x \in \{0,1\}^n \mid f_i(x) = 0 \text{ かつ } f_j(x) = 1\}$ の上側の共通部分を U とおいた上で, U の極小元 u に注目すれば, 容易に証明することができる. より詳しくは, u の「直ぐ下にあるベクトル」全てからなる集合, つまり, x と y の間のハミング距離を $d_H(x,y)$ と表したとき $\{x \in \{0,1\}^n \mid x \leq u \text{ かつ } d_H(x,u) = 1\}$ と表される集合を W とおけば,

$$W \subseteq X \cup Y,$$

$$W \cap X \neq \emptyset \quad \text{かつ} \quad W \cap Y \neq \emptyset$$

を導くことができる. 補題 1 の証明の詳細は省略する.

但し, 上の定理 4 からは, $\mathcal{G}_n$ に属する関数で $\mathcal{G}_n$ によっても $\mathcal{G}_n$ と $\mathcal{C}_n$ によっても分解不可能なものは, 基本素子集合に属することが保証されるが, それ以外の関数を含む基本素子集合が存在する可能性は否定できない. 例えば, 次の予想が成立すれば, そのような基本素子集合は存在せず, 従って, 基本素子集合が一意に定まることになる.

予想 2 f および g を n 変数単調並べ換え関数とする. $g \circ f$ と f が同値でないならば,

$$|(g \circ f)(\{0,1\}^n)| < |f(\{0,1\}^n)|$$

が成立する.

参考文献

[1] M. Ajtai, J. Komlós, and E. Szemerédi. An $O(n \log n)$ sorting network. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing*, pages 1–9, 1983.

[2] M. Ajtai, J. Komlós, and E. Szemerédi. Sorting in $c \log n$ parallel steps. *Combinatorica*, 3 (1):1–19, 1983.

[3] R.L. Graham. A mathematical study of a model of magnetic domain interactions. *Bell Syst. Tech. J.*, 49 (8):1627–1644, 1970.

[4] D. E. Knuth. *The art of computer programming, Sorting and searching*, volume 3. Addison-Wesley, 1973.

[5] I. Parberry. A computer-assisted optimal depth lower bound for nine-input sorting networks. *Math. Systems Theory*, 24:101–116, 1991.